Galois Categories and the Étale Fundamental Group

Swayam Chube

April 27, 2025

§1 Preliminaries on Profinite Groups

Proposition 1.1. Let π be a profinite group acting on a set E. Then

- (1) The action is continuous if and only if for each $e \in E$, $\operatorname{Stab}_{\pi}(e)$ is open in π .
- (2) If E is finite, the action is continuous if and only if its kernel $\{\sigma \in \pi : \sigma e = e \ \forall \ e \in E\}$ is open in π .
- (3) Any finite transitive π -set is isomorphic to π/π' for a certain open subgroup π' of π .

Proof. (1) If the action is continuous, then the function $\pi \to E$ given by $\sigma \mapsto \sigma e$ is continuous and the preimage of e, which is precisely the stabilizer of e in π , is open.

Conversely, suppose every stabilizer is open. Let $A:\pi\times E\to E$ denote the action. Since E is discrete, it suffices to show that $A^{-1}(e)$ is open for each $e\in E$. Let $e'\in\pi\cdot e$ and suppose $\tau_{e'}\in\pi$ is such that $\tau_{e'}e=e'$. Then

$$\{\sigma \colon \sigma e' = e\} = \tau_{e'}^{-1} \operatorname{Stab}_{\pi}(e'),$$

which is an open subset of π . Consequently,

$$\mathcal{A}^{-1}(e) = \bigcup_{e' \in \pi \cdot e} \left\{ (\sigma, e') \colon \sigma e' = e \right\} = \bigcup_{e' \in \pi \cdot e} \tau_{e'}^{-1} \operatorname{\mathsf{Stab}}_{\pi}(e') \times \{e'\}$$

is an open subset of $\pi \times E$, as desired.

(2)

§2 Galois Categories

§§ Statement of the Main Theorem

Definition 2.1. Let $\mathscr C$ be a category, X an object of $\mathscr C$, and G a subgroup of $\operatorname{Aut}_{\mathscr C}(X)$. The *quotient* of X by G is an object X/G of $\mathscr C$ together with a morphism $p:X\to X/G$ satisfying

- (i) $p = p \circ \sigma$ for all $\sigma \in G$,
- (ii) if $X \xrightarrow{f} Y$ is a morphism in $\mathscr C$ such that $f = f \circ \sigma$ for all $\sigma \in G$, then there is a unique morphism $X/G \xrightarrow{g} Y$ making



commute.

The quotient of an object by a group need not exist in a category, but when it does, it must be unique up to a unique isomorphism.

Definition 2.2. Let $\mathscr C$ be a category and $F:\mathscr C\to \textbf{FinSets}$ a (covariant) functor from $\mathscr C$ to the category of finite sets. We say that the pair $(\mathscr C,F)$ is a *Galois category*, or that $\mathscr C$ is a Galois category with *fundamental functor F*, if the following axioms are satisfied:

- (G1) There is a terminal object and $\mathscr C$ admits all fibred products.
- **(G2)** An initial object exists in \mathscr{C} , finite coproducts exist in \mathscr{C} , and for any object in \mathscr{C} , the quotient by a finite group of automorphisms exists.
- **(G3)** Any morphism u in $\mathscr C$ factors as $u=u'\circ u''$ where u' is a monomorphism and u'' is an epimorphism. Every monomorphism $X\stackrel{f}{\to} Y$ in $\mathscr C$ is an isomorphism of X with a direct summand of Y; i.e., there is an object $Z\stackrel{g}{\to} Y$ such that



is a coproduct diagram.

- (G4) The functor F sends terminal objects to terminal objects and commutes with fibred products.
- (G5) The functor F sends initial objects to initial objects, commutes with finite coproducts, sends epimorphisms to epimorphisms, and commutes with passage to the quotient by a finite group of automorphisms.
- **(G6)** If u is a morphism in $\mathscr C$ such that F(u) is an isomorphism, then u is an isomorphism.

Proposition 2.3. Let (\mathscr{C}, F) be a small Galois category and set $\mathscr{D} = [\mathscr{C}, \mathbf{FinSets}]$, the functor category between \mathscr{C} and the category of finite sets. Then $\mathrm{Aut}_{\mathscr{D}}(F)$ is a profinite group acting continuously on F(X) for every $X \in \mathscr{C}$.

Proof. An element of $\operatorname{Aut}_{\mathscr{D}}(F)$ is a natural isomorphism $\eta: F \Rightarrow F$, i.e, each $\eta_X: F(X) \to F(X)$ is an isomorphism. Hence, we can identify $\operatorname{Aut}_{\mathscr{D}}(F)$ with a subgroup of $\prod_{X \in \mathscr{C}} \mathfrak{S}_{F(X)}$, where $\mathfrak{S}_{F(X)}$ is the group of permutations of F(X). In particular,

$$\operatorname{Aut}_{\mathscr{D}}(F) = \left\{ (\eta_X)_X \in \prod_{X \in \mathscr{C}} \mathfrak{S}_{F(X)} \colon \text{ for each } Y \xrightarrow{f} Z \text{ in } \mathscr{C}, \ \eta_Z \circ F(f) = F(f) \circ \eta_Y \right\}.$$

2

Let $Y \xrightarrow{f} Z$ be a morphism in \mathscr{C} . Then the set

$$\mathfrak{A}_f = \left\{ (\eta_X)_X \in \prod_{X \in \mathscr{C}} \mathfrak{S}_{F(X)} \colon \eta_Z \circ F(f) = F(f) \circ \eta_Y \right\}.$$

is closed, as it is the finite union of the closed sets

$$\prod_{\substack{X \in \mathscr{C} \\ X \neq Y \ Z}} \mathfrak{S}_{F(X)} \times \{\eta_Y\} \times \{\eta_Z\},\,$$

where $\eta_Y \in \mathfrak{S}_{F(Y)}$ and $\eta_Z \in \mathfrak{S}_{F(Z)}$ satisfy $\eta_Z \circ F(f) = F(f) \circ \eta_Y$. Now, since

$$\operatorname{\mathsf{Aut}}_{\mathscr{D}}(F) = \bigcap_{\substack{Y \stackrel{f}{\longrightarrow} Z \ \text{in }\mathscr{C}}} \mathfrak{A}_f,$$

it is a closed subgroup of $\prod_{X \in \mathcal{S}} \mathfrak{S}_{F(X)}$, so that it is a profinite group.

Finally, the map $\operatorname{Aut}_{\mathscr{D}}(F) \times F(X) \to F(X)$ given by $((\eta_X)_{X \in \mathscr{C}}, a) \longmapsto \eta_X(a)$ defines an action of $\operatorname{Aut}_{\mathscr{D}}(F)$ on F(X). The stabilizer of each $a \in F(X)$ is precisely

$$\operatorname{\mathsf{Aut}}_{\mathscr{D}}(F) imes \left(\prod_{\substack{Y \in \mathscr{C} \\ Y
eq X}} \times \operatorname{\mathsf{Stab}}_{\mathfrak{S}_{F(X)}}(a) \right),$$

which is an open subgroup of $Aut_{\mathscr{D}}(F)$. Due to Proposition 1.1, this action is continuous.

Interlude 2.4 (Construction of the Main Functor). Let (\mathscr{C},F) be a small Galois category. Define the functor $H:\mathscr{C}\to \operatorname{Aut}(F)$ -sets sending each $X\in\mathscr{C}$ to F(X) with the $\operatorname{Aut}(F)$ -action as defined in the proof of Proposition 2.3. If $Y\stackrel{f}\to Z$ is a morphism in \mathscr{C} , then the induced morphism $F(f):F(Y)\to F(Z)$ is $\operatorname{Aut}(F)$ -linear: indeed, if $\eta=(\eta_X)_X\in\operatorname{Aut}(F)$, then for $y\in Y$,

$$F(f)(\eta y) = F(f)(\eta_Y y) = \eta_Z(F(f)(z)) = \eta F(f)(z).$$

Theorem 2.5 (Fundamental Theorem of Galois Categories). Let (\mathscr{C}, F) be an essentially small Galois category. Then

- (1) The functor $H: \mathscr{C} \to \operatorname{Aut}(F)$ -sets is an equivalence of categories.
- (2) If π is a profinite group such that the categories $\mathscr C$ and π -sets are equivalent by an equivalence, that when composed with the forgetful functor π -sets \to FinSets yields the funtor F, then π is canonically isomorphic to $\operatorname{Aut}(F)$.
- (3) If F' is a second fundamental functor on \mathscr{C} , then F and F' are naturally isomorphic.
- (4) If π is a profinite group such that the categories $\mathscr C$ and π -sets are equivalent, then there is an isomorphism of profinite groups $\pi \cong \operatorname{Aut}(F)$ that is canonically determined up to an inner automorphism of $\operatorname{Aut}(F)$.

Henceforth, let
$$(\mathscr{C}, F)$$
 be a small Galois category.

§§ Subobjects and connected objects

Definition 2.6. Lt $X \in \mathscr{C}$. Consider the set $\{Y \to X \text{ a monomorphism}\} / \sim \text{ where}$

$$Y \xrightarrow{f} X \sim Y' \xrightarrow{f'} X$$

if and only if there is an isomorphism $Y \xrightarrow{\cong} Y'$ making

$$Y \xrightarrow{\cong} Y'$$

$$f \downarrow \qquad \qquad f'$$

$$X$$

commute. Every equivalence class in the above is called a *subobject* of X.

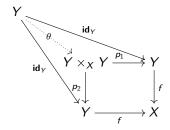
Lemma 2.7. f is a monomorphism if and only if F(f) is injective.

Proof. Let $Y \xrightarrow{f} X$. We first show that f is a monomorphism if and only if the canonical map $p_1: Y \times_X Y \to Y$ is an isomorphism. If f is a monomorphism, then it is clear that Y = Y is a coproduct diagram, so that



 $p_1: Y \times_X Y \to Y$ is an isomorphism.

Conversely, suppose $p_1: Y \times_X Y \to Y$ is an isomorphism and consider the commutative diagram



Since p_1 is an isomorphism, it follows that $\theta = p_1^{-1}$ is an isomorphism. Further, since $p_2 \circ \theta = id_Y$, we must have that $p_1 = p_2$.

Now, suppose $h_1, h_2: Z \to Y$ are morphisms in $\mathscr C$ satisfying $f \circ h_1 = f \circ h_2$, then there is a morphism $\varphi: Z \to Y \times_X Y$ making the required diagram commute. But then

$$h_1 = p_1 \circ \varphi = p_2 \circ \varphi = h_2$$
,

so that f is a monomorphism.

Coming back to the proof of the Lemma, we have

$$F(f)$$
 is injective $\iff F(f)$ is a monomorphism $\iff F(p_1)$ is an isomorphism $\iff p_1$ is an isomorphism $\iff f$ is a monomorphism,

where the first equivalence follows from the classification of monomorphisms in **FinSets**, the second and last equivalences follow from what we just proved and (G4), and the third isomorphism follows from (G6).

Lemma 2.8. Two monomorphisms $Y \xrightarrow{f} X$ and $Y' \xrightarrow{f'} X$ are representative of the same subobject of X if and only if F(f)(F(Y)) = F(f')(F(Y')) as subsets of F(X).

Proof. Suppose the two objects represent the same subobject of X. Then there is an isomorphism $\theta: Y \xrightarrow{\sim} Y'$ such that $f = f' \circ \theta$. Then, $F(f)(F(Y)) = F(f') \circ F(\theta)(F(Y))$ but $F(\theta)$ is an isomorphism, so is surjectiv,e and hence F(f)(F(Y)) = F(f')(F(Y')).

Conversely, suppose F(f)(F(Y)) = F(f')(F(Y')). As F commutes with fibred products, we have the following pullback squares

$$\begin{array}{cccc} Y \times_X Y' \xrightarrow{p_1} Y & F\left(Y \times_X Y'\right) \xrightarrow{F(p_1)} Y \\ & \downarrow f & F(p_2) \downarrow & \downarrow F(f) \\ Y' \xrightarrow{f'} X & Y' \xrightarrow{F(f')} X \end{array}$$

Since the latter is a pullback square, we have

$$F(Y \times_X Y') = \{(y, y') \in F(Y) \times F(Y') : F(f)(y) = F(f')(y')\}.$$

As F(f) and F(f') are injective with the same image in X, it is clear that both $F(p_1)$ and $F(p_2)$ must be bijections, consequently, due to (G6), both p_1 and p_2 must be isomorphisms isomorphisms in \mathscr{C} . Finally, this gives $f = f' \circ (p_2 \circ p_1^{-1})$, as desired.

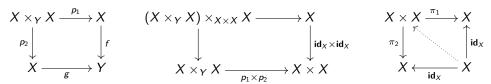
Definition 2.9. An object $X \in \mathscr{C}$ is said to be *connected* if it has exactly two subobjects, $0 \to X$ and $id_X : X \to X$. **Proposition 2.10.** Every object in $\mathscr{C} \neq 0$ is the coproduct of its connected subobjects.

Proof. Let X be a non-initial object in $\mathscr C$. We shall argue by induction on #F(X). If #F(X)=1, then X is connected, for if $Y\stackrel{f}{\to} X$ is a subobject, then $F(Y)\stackrel{F(f)}{\longrightarrow} F(X)$ is injective, so that $F(Y)=\emptyset$ or F(Y)=F(X). In the latter case, F(f) is an isomorphism and hence, so is f; on the other hand, if $F(Y)=\emptyset$, then Y must be the initial object of $\mathscr C^1$. Suppose now that $\#F(X)\geqslant 2$; since there is nothing to prove when X is connected, we may suppose that X is not connected. Then there is a subobject $Y\stackrel{q_1}{\to} X$ of X which is neither initial, nor an isomorphism. Due to (G3), there is a morphism $Z\stackrel{q_2}{\to} X$ such that $X=Y\coprod Z$. This coproduct diagram transforms into a coproduct diagram in **FinSets**, so that $F(q_2)$ is injective, consequently due to Lemma 2.7, $F(q_2)$ is a monomorphism. It follows that $F(q_2)$ is another subobject of $F(q_2)$ is finite, it is clear that this is a finite coproduct.

It remains to show that X is the disjoint union of each of its connected subobjects. Suppose $X = \coprod_{i=1}^n X_i$ and Y a connected subobject of X. I shall treat F(Y) and $F(X_i)$ as subsets of F(X) for ease of notation. Since $F(X) = \coprod_i F(X_i)$, there is some index j such that $F(Y) \times_{F(X)} F(X_j) = F(Y) \cap F(X_j) \neq \emptyset$. As a result, $Y \times_X X_j$ is not the initial object of $\mathscr C$. Since $F(Y \times_X X_j) \to F(X_j)$ and $F(Y \times_X X_j) \to F(Y)$ are injective, due to Lemma 2.7, the maps $Y \times_X X_j \to X_j$ and $Y \times_X X_j \to Y$ must be monomorphisms, and hence, must be isomorphisms. It follows that X_j and Y are the same subobject of X.

Lemma 2.11. \mathscr{C} admits all equalizers.

Proof. Let $f, g: X \to Y$ be morphisms in \mathscr{C} . There are two fibred product diagrams



We claim that $W = (X \times_Y X) \times_{X \times X} X \to X$ is the equalizer of f and g. Clearly, we have the following equality of compositions:

$$W \to X \xrightarrow{f} Y = W \to X \xrightarrow{\operatorname{id}_X} X \xrightarrow{f} Y$$

$$= W \to X \to X \times X \xrightarrow{\pi_1} X \xrightarrow{f} Y$$

$$= W \to X \times_Y X \to X \times X \xrightarrow{\pi_1} X \xrightarrow{f} Y$$

$$= W \to X \times_Y X \xrightarrow{p_1} X \xrightarrow{f} Y$$

$$= W \to X \times_Y X \xrightarrow{p_2} X \xrightarrow{g} Y$$

$$= W \to X \times_Y X \to X \times X \xrightarrow{\pi_2} X \xrightarrow{g} Y$$

$$= W \to X \xrightarrow{\operatorname{id}_X} X \xrightarrow{g} Y$$

$$= W \to X \xrightarrow{\operatorname{id}_X} X \xrightarrow{g} Y$$

$$= W \to X \xrightarrow{g} Y.$$

¹Indeed, if 0 is "the" initial object of \mathscr{C} , then there is a unique morphism $0 \xrightarrow{u} Y$ in \mathscr{C} . But since F(u) is an isomorphism in **FinSets**, it follows from (G6) that u is an isomorphism.

If $h: Z \to X$ is such that $f \circ h = g \circ h$, then there is a unique map $\theta: Z \to X \times_Y X$ induced by $Z \xrightarrow{h} X$, which then induces a unique map $\phi: Z \to W$, as desired.

Proposition 2.12. Let A be a connected object in \mathscr{C} and $a \in F(A)$. Then for every $X \in \mathscr{C}$, the map

$$\mathscr{C}(A,X) \longrightarrow F(X) \qquad f \longmapsto F(f)(a)$$

is injective.

Proof. Let $f,g \in \mathscr{C}(A,X)$ be such that F(f)(a) = F(g)(a), and let (C,θ) be the equalizer of f,g, which is known to exist due to Lemma 2.11. Since F commutes with fibred products, it must commute with equalizers too, hence $(F(C), F(\theta))$ is an equalizer of $F(f), F(g) : F(A) \to F(X)$. In particular, $F(\theta)$ is injective, so that θ is a monomorphism due to Lemma 2.7. Moreover,

$$a \in F(C) = \{b \in F(A) \colon F(f)(b) = F(g)(b)\} \neq \emptyset,$$

and hence C is not the initial object of \mathscr{C} , whence $\theta: C \to A$ is an isomorphism, which implies f = g.

Interlude 2.13. Consider the set $I = \{(A, a): A \text{ connected}, a \in F(A)\} / \sim \text{ where } \sim \text{ is the equivalence relation:}$

$$(A, a) \sim (B, b) \iff \exists f : A \rightarrow B \text{ an isomorphism such that } F(f)(a) = b.$$

We can define a partial order on I by

$$(A, a) \ge (B, b) \iff \exists f : A \to B \text{ a morphism such that } F(f)(a) = b.$$

Note that due to Proposition 2.12 the above map f, if it exists, is unique. We claim that (I, \geq) is a directed set under this order relation:

Reflexivity: Taking $f = id_A$, we have $F(id_A)(a) = a$, so $(A, a) \ge (A, a)$.

Anti-symmetry: If $(A, a) \ge (B, b)$ and $(B, b) \ge (A, a)$, then there are morphisms $A \xrightarrow{f} B$ and $B \xrightarrow{g} A$ such that F(f)(a) = b and F(g)(b) = a. Consequently, $F(g \circ f)(a) = a$ and $F(f \circ g)(b) = b$. Using Proposition 2.12, it follows that $g \circ f = \mathbf{id}_A$ and $f \circ g = \mathbf{id}_B$, that is, (A, a) = (B, b).

Transitivity: If $(A, a) \ge (B, b) \ge (C, c)$ and $A \xrightarrow{f} B$ and $B \xrightarrow{g} C$ are the corresponding maps, then $g \circ f : A \to C$ is such that

$$F(g \circ f)(a) = F(g) \circ F(f)(a) = F(g)(b) = c.$$

Directedness: Let $(A, a), (B, b) \in I$. Choose a connected subobject $C \to A \times B$ such that the image of F(C) in $F(A \times B) = F(A) \times F(B)$ contains $a \times b$; further, let $c \in C$ be the unique element in F(C) mapping to $a \times b$. Compose the monomorphism $C \to A \times B$ with the canonical projections $A \times B \xrightarrow{p_1} A$ and $A \times B \xrightarrow{p_2} B$ to obtain maps f_1 and f_2 . Then it is clear that $F(f_1)(c) = a$ and $F(f_2)(c) = b$, so that $(C, c) \supseteq (A, a), (B, b)$.

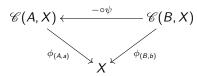
We shall write $(A, a) \ge_f (B, b)$ if we want to specify the morphism $A \xrightarrow{f} B$ satisfying F(f)(a) = b.

If $(A, a) \ge_f (B, b)$, then the morphism $f : A \to B$ induces a natural transformation of functors $\mathscr{C}(B, -) \xrightarrow{-\circ f} \mathscr{C}(A, -)$. This gives us a projective system of functors in the functor category $[\mathscr{C}, \mathsf{FinSets}]$.

Theorem 2.14. There is an isomorphism of functors

$$\varinjlim_{(A,a)\in I}\mathscr{C}(A,-)\longrightarrow F(-)\qquad f\longmapsto F(f)(a)$$

Proof. Consider the maps $\phi_{(A,a)}: \mathscr{C}(A,X) \to F(X)$ given by $f \mapsto F(f)(a)$. If $(A,a) \geq_{\psi} (B,b)$, then it is clear that the diagram



commutes. This clearly induces a map $\phi: \varinjlim_{(A,a)\in I} \mathscr{C}(A,X) \to F(X)$ given by

$$\phi(f) = \phi_{(A,a)}(f)$$
 if $f \in \mathscr{C}(A, X)$.

It suffices to show that this map is a bijection of sets, since then it would follow that ϕ is an isomorphism of functors.

First, we show injectivity. Suppose F(f)(a) = F(g)(b) for some $(A, a), (B, b) \in I$ and $f \in \mathcal{C}(A, X)$ and $g \in \mathcal{C}(B, X)$. Let $C \to A \times B$ be a connected subobject such that $(a, b) \in f(C)$, and let p'_1, p'_2 be the compositions of the projection maps $p_1 : A \times B \to A$ and $p_2 : A \times B \to B$ with the monomorphism $C \to A \times B$. It is then clear that $(C, C) \supseteq (A, a)$ and $(C, C) \supseteq (B, b)$.

Under the map $\mathscr{C}(A,X) \to \mathscr{C}(C,X)$, the morphism f maps to $f \circ p_1'$ and under the map $\mathscr{C}(B,X) \to \mathscr{C}(C,X)$, the morphism g maps to $g \circ p_2'$. We contend that these two maps are the same. Indeed, since $F(fp_1')(c) = F(gp_2')(c)$, due to Proposition 2.12, $fp_1' = gp_2'$. This shows that f and g are equal in $\varinjlim_{(A,a) \in I} \mathscr{C}(A,X)$.

Finally, to see surjectivity, take $x \in F(X)$ and consider $f: A \to X$, the connected component of X such that $x \in F(A)$. Then $(A, x) \in I$ and F(f)(x) = x. This completes the proof.

§§ Galois Objects

If A is a connected object, then we have the inequalities:

$$\# \operatorname{Aut}_{\mathscr{C}}(A) \leqslant \# \mathscr{C}(A, A) \leqslant \# F(A),$$

where the second inequality follows from Proposition 2.12. In particular, the set of automorphisms of A is finite, and therefore, it makes sense to talk about the quotient of a connected object by its group of automorphisms.

Definition 2.15. An object $A \in \mathcal{C}$ is called a *Galois object* if $A / Aut_{\mathcal{C}}(A)$ is a terminal object.

Proposition 2.16. Let $X \in \mathscr{C}$. There exists $(A, a) \in I$ with A Galois such that the map $\mathscr{C}(A, X) \to F(X)$ given by $f \mapsto F(f)(a)$ is bijective.

Proof. Let $Y = X^{\#F(X)}$ be the product of #F(X) copies of X. As F commutes with products, we have $F(Y) = F(X)^{\#F(X)}$. Let us index the coordinates of Y by the elements of F(X), and let $A \in F(Y)$

Remark 2.17. The above result shows that the subset $J \subseteq I$ corresponding to connected Galois objects is a cofinal subset of I, so

$$\lim_{\longrightarrow} \mathscr{C}(A,-) \cong \lim_{\longrightarrow} \mathscr{C}(A,-) \cong F.$$

§§ Construction of the Equivalence

Lemma 2.18. Let A be a connected Galois object, and B a connected object such that $\mathscr{C}(A, B) \neq \emptyset$. Then, the action

$$\operatorname{Aut}_{\mathscr{C}}(A) \times \mathscr{C}(A, B) \to \mathscr{C}(A, B) \qquad (\sigma, f) \mapsto f \circ \sigma$$

is transitive.

Proof. Let $f \in \mathcal{C}(A, B)$, then we can factor f = gh where h is an epimorphism and g is a monomorphism. Since B is connected, g must be an isomorphism since both A and B are connected. In particular, this means that F(f) is an isomorphism. Thus, given $f': A \to B$, there exists an $a' \in F(A)$ such that F(f)(a') = F(f')(a). Since A is Galois, there exists a unique $\sigma \in \operatorname{Aut}_{\mathcal{C}}(A)$ such that $F(\sigma)(a) = a'$. Then $F(f\sigma)(a) = F(f')(a)$, and due to Proposition 2.12, we have that $f \circ \sigma = f'$.

Lemma 2.19. Let $(A, a), (B, b) \in J$, $(A, a) \ge_f (B, b)$. Given $\sigma \in \operatorname{Aut}_{\mathscr{C}}(A)$, there exists a unique $\tau \in \operatorname{Aut}_{\mathscr{C}}(B)$ such that $\tau \circ f = f \circ \sigma$ and the mapping $\sigma \mapsto \tau$ is a surjective group homomorphism $\operatorname{Aut}_{\mathscr{C}}(A) \to \operatorname{Aut}_{\mathscr{C}}(B)$.

Proof. Let $a' := F(\sigma)(a)$ and b' := F(f)(a'). Then, since B is Galois, there exists a unique $\tau \in \operatorname{Aut}_{\mathscr{C}}(B)$ such that $F(\tau)(b) = b'$ due to Proposition 2.16. So, we have

$$F(f\sigma)(a) = b' = F(\tau f)(a) \implies f \circ \sigma = \tau \circ f$$

due to Proposition 2.12. It remains to show that such a $\tau \in \operatorname{Aut}_{\mathscr{C}}(B)$ is unique. Indeed, if there were two automorphisms $\tau_1, \tau_2 \in \operatorname{Aut}_{\mathscr{C}}(B)$ satisfying the property, i.e., $\tau_1 \circ f = f \circ \sigma = \tau_2 \circ f$, then $F(\tau_1)(b) = F(\tau_2)(b)$. Due to Proposition 2.12, it follows that $\tau_1 = \tau_2$.

Finally, we must show that the association $\sigma \mapsto \tau$ is a surjective group homomorphism $\operatorname{Aut}_{\mathscr{C}}(A) \to \operatorname{Aut}_{\mathscr{C}}(B)$. Indeed, if $\sigma_1 \mapsto \tau_1$ and $\sigma_2 \mapsto \tau_2$, then we have

$$f\sigma_1\sigma_2=\tau_1f\sigma_2=\tau_1\tau_2f,$$

and so $\sigma_1\sigma_2 \mapsto \tau_1\tau_2$. This proves that the association $\sigma \mapsto \tau$ is a group homomorphism. Further, due to Lemma 2.18, the action of $\operatorname{Aut}_{\mathscr{C}}(A)$ on $\mathscr{C}(A,B)$ is transitive, and hence, given $\tau \in \operatorname{Aut}_{\mathscr{C}}(B)$, there exists a $\sigma \in \operatorname{Aut}_{\mathscr{C}}(A)$ such that $\tau \circ f = f \circ \sigma$, whence the association $\sigma \mapsto \tau$ is surjective, thereby completing the proof.